Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

Novel Encryption and Decryption Technique Using ATP & New Sequent Rules in Three Variables

[1] **K. Kanthi Sowjanya,** [*] [2]**Talari Surendra,** [3]**Suryaprakash Nalluri**, [4]**V.Sree Ramani**, [5]**Subrahmanya S Meduri**, [6]**P S V S Sridhar**,

[1]*Research Scholar, Department of Mathematics, GSS, GITAM Deemed to be University, Visakhapatnam - 45, Andhra Pradesh, India*

[2]*Department of Mathematics, GSS, GITAM Deemed to be University, Visakhapatnam - 45, Andhra Pradesh, India*

[3]*Department - Information Security, Affiliation-University of Cumberland,Williamsburg, USA*

[4]*Department of mathematics, Chaitanya Bharati Institute of Technology, Gandipet-500075, Telangana, India*

[5]*Technical Architect, Wipro Technologies, USA*

[6]*Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India*

Abstract:-The act of safeguarding digital information from unauthorized access, corruption or theft is called Data Security. The secured encryption and decryption method gives more security from unauthorized access. Here we developed a new Encryption and Decryption technique using ATP (Automatic Theorem Proving) and new antecedent & consequent rules in three variables assigned with conversion systems. As it involves various degrees of encryptions and decryptions, the security is more and this technique is infeasible to attacks.

Keywords:ATP, New antecedent rules,New consequent rules, Encryption, Decryption and Security**.**

1. Introduction

This paper discusses novel encryption and decryption method using Automatic Theorem Proving and new sequent rules in two and three variables with connectives. In this method, the difficulty of the technique depends on number elements in the domain set. The number of elements in the domain set is directly proportional to the length the block.

T. Surendra et al. [21] proposed cryptosystem developed by ATP and sequent rules assigned by existing ciphers is very feasible for the attackers even thought it contains various levels of encryptions and decryptions.

T. Surendra et al. [22] proposed cryptosystem developed by ATP and new sequent rules in two variable and new ciphers is infeasible for the attackers as the sequent rules assigned by new ciphers, which contain alphabets.

We proposed in this paper a novel crypto system using ATP and new developed antecedent and consequent rules in three variables. Which are treating as encryption and decryption rules. For these developed sequent rules we assigned various number conversion system such as Binary Number System, Octal number system, Hexadecimal number system and ASCII Number System for these variables. For two variable sequent rules we used [22] new developed ciphers such as Tree fence technique, Slash fair cipher, Jelly cipher, Triangular cipher and Passing key cipher. Since this cryptosystem contain various levels of encryption, decryption, it is very difficult to the attacker to decrypt the plain text. So security levels are more and for attackers, it is infeasible [19,23].

1.1 Description of Automatic Theorem Proving: [2]

To check the validity of a given statement from the set of premises, Automatic Theorem Proving which includes antecedent rules, consequent rules, sequent, axioms, statements, premises is used. To build each step of derivation in a specific method without any barrier to any ingenuity and finally arriving at the last step, set of rules and procedure are followed. In spite of being a mechanical procedure, more than any other previously available methods, it is an exponential procedure for the verification of the validity of the statement/conclusion. This system includes the procedures of techniques of derivation like 10 rules, an axiom schema and rules of well-formed sequent & formulas and is more competent than the previous methods.

1. The capital letters K, L, M…. used as statement variables and statement formulas are considered to be the variables.
2. The connectives appear in the formulas with the order of precedence as given.
3. String of formulas: A string of formulas is defined as follows:

(a) Any formula is considered a string of formulas
(b) If alpha and beta are strings of formulas, then alpha-beta and beta-alpha are the strings of formulas
(c) Only those strings obtained by steps (a) and (b) are considered strings of formulas, with the exception of the empty string which is also a string of formulas.

Note: The order in which the formulas appear in a string is not significant and hence, the strings P, Q, R; Q, R, P; P, R, Q; etc., are the same.

4. Sequent: If alpha and beta are strings of formulas, they are called a *sequent* in which alpha is denoted as the antecedent and beta as the consequent of the sequent.

Thus P, Q, R, S, T, U is true if and only if PQRSTU is true. i.e., A sequent is true if and only if either at least one of the formulas of the antecedent is false or at least one of the formulas of the consequent is true. Hence, the symbol is a generalization of the connection to strings of formulas. Similarly, the symbol applied to the strings of formulas is used as a generalization of the symbol. Thus P⇒Q means “P implies Q” or is a tautology which means that is true. Ex: X, Y, Z⇒^{S}X, N

The empty antecedent is described as the logical constant “true” (T) and the empty consequent is described as the logical constant “false” (F).

5. Axiom Schema: If alpha and beta are strings of formulas such that every formula in both alpha and beta is a variable only, then the sequent is an axiom if and only if alpha and beta have at least one variable in common.

Ex: M, N, O⇒^{S}X, N, Y is an axiom, where M, N, O, X&Y are variables

6. Theorem: The following sequents are theorems of our system

(a) Every axiom is a theorem.
(b) If a sequent alpha is a theorem and a sequent beta result from alpha through the use of one of the above rules of the system, then beta is a theorem.
(c) Sequents obtained by (a) and (b) are the only theorems.

1.2 Rules:

1.2.1 Rules for two variables : [21, 22]

To combine formulas within strings we used following set of connectives {**@,Θ,®,©,ö**}. Corresponding to each of these connectives there are two rules, one for the introduction of the connective in the antecedent and the other for its introduction in the consequent. The strings of formulas while P and Q are formulas to which the connectives are applied [24] in the description of these enhanced antecedent and consequent rules.

Antecedent Rules:

1. Rule ¬ ⇒ : If a1, a2 ⇒ A, a3 then a1, ¬A, a2 ⇒ a3
2. Rule ∧ ⇒ : If A, B, a1, a2 ⇒ η, then a1, A ∧B, a2 ⇒ a3

3. Rule $\vee \Rightarrow$: If A, a1, a2 $\Rightarrow$ a3 and B, a1, a2 $\Rightarrow$ a3, then a1, A$\vee$B, a2 $\Rightarrow$ a3
4. Rule $\rightarrow \Rightarrow$: If B, a1, a2 $\Rightarrow$ a3 and a1, a2 $\Rightarrow$ A, a3, then a1, A$\rightarrow$B, a2$\Rightarrow$ a3
5. Rule $\leftrightarrow \Rightarrow$: If A,B, a1, a2$\Rightarrow$ a3 and a1, a2$\Rightarrow$A, B, a3, then a1, A$\leftrightarrow$B, a2$\Rightarrow$a3

where A,B,a1,a2 & a3 are atomic variables of compound statements.

Defined Antecedent Rules for two variables:

6. Rule @ $\Rightarrow$: If A1,AB, A2$\Rightarrow$B, A3 then A1,A@B, A2 $\Rightarrow$ A3
7. Rule Θ $\Rightarrow$: If A1,A,A2 $\Rightarrow_{AB,}$A3 then A1,AΘB, A2 $\Rightarrow$ A3
8. Rule ® $\Rightarrow$: If A1,B, A2$\Rightarrow_{BA,}$ A3 then A1,A®B, A2 $\Rightarrow$ A3
9. Rule © $\Rightarrow$: If A1,BA, A2$\Rightarrow_{A,}$ A3 then A1,A©B, A2$\Rightarrow$ A3
10. Rule ö $\Rightarrow$: If A1,B, A2$\Rightarrow_{AB,}$ A3 then A1,Aö B, A2$\Rightarrow$ A3

where A,B,A1,A2 & A3 are atomic variables of compound statements. [17,18]

Defined Antecedent Rules for three variables:

1. K1,(X_1¤X_2)ȺX_3, K2$\Rightarrow^S$ k3 then K1,$X_1X_2X_3$,K2 $\Rightarrow$K3

2. K1,(X_1ƧX_2)ጠX_3,K2 $\Rightarrow^S$ K3 then K1,X_1, K2$\Rightarrow$ K1,X_2X_3, K2

3. K1,(X_1ƃX_2)∀X_3, K2$\Rightarrow^S$ then K1,X_1X_3, K2$\Rightarrow X_2$,K3

where X_1,X_2,X_3,K1,K2 & K3 are atomic variables of compound statements.

Consequent Rules: [21]

1. Rule $\Rightarrow \neg$: If A, A1 $\Rightarrow$ A2, A3 then A1$\Rightarrow$A2, $\neg$A, A3
2. Rule$\Rightarrow \wedge$: If A1$\Rightarrow$A, A2, A3 and A1$\Rightarrow$B, A2, A3, then A1$\Rightarrow$A2, A$\wedge$B, A3
3. Rule$\Rightarrow \vee$: If A1$\Rightarrow$A, B, A2, A3 then A1 $\Rightarrow$ A2, A$\vee$B, A3
4. Rule$\Rightarrow \rightarrow$: If A, A1$\Rightarrow$B, A2, A3 then A1$\Rightarrow$A2, A$\rightarrow$B, A3
5. Rule $\Rightarrow \leftrightarrow$: If A, A1$\Rightarrow$B, A2, A3 and B, A1$\Rightarrow$A, A2, A3 then A1$\Rightarrow$A2, A$\leftrightarrow$B, A3

where A,B,A1,A2 & A3 are atomic variables of compound statements. [14,15]

Defined Consequent Rules for two variables : [22]

1. Rule $\Rightarrow$@: If A1,B$\Rightarrow$A, A2, A3 then A1$\Rightarrow$ A2,A@B,A3

2. Rule$\Rightarrow$Θ: If A1,A$\Rightarrow$ A2,BA,A3 then A1$\Rightarrow$A2,AΘB, A3

3. Rule$\Rightarrow$®: If A1,B$\Rightarrow$A2,AA,A3 then A1$\Rightarrow$A2,A®B,A3

4. Rule$\Rightarrow$©: If A1$\Rightarrow$ A2,BA,A3 then A1$\Rightarrow$A2,A©B,A3

5. Rule $\Rightarrow$ö: If A1$\Rightarrow$ A1,AB,A3and A1$\Rightarrow$A,A2,A3 then A1$\Rightarrow$A2,Aö B,A3

where A,B,A1,A2 & A3 are atomic variables of compound statements. [9,11]

Defined Consequent Rules for three variables :

1. K1$\Rightarrow^S$ K2 ,(X_1¤X_2)Ⱥ X3, K3 thenK1$\Rightarrow$K1,X_1X_2 X_3,K3

2. K1$\Rightarrow^S$ K2, (X_1ƧX_2) ጠ X_3 , K3 then K1,X_1X_2, K2 $\Rightarrow X_3$,K3

3. K1$\Rightarrow^S$K2,(X_1ƃX_2)∀X3,K3 then K1,X2,K2 $\Rightarrow$K1,X_1X_3,K3

where X_1,X_2,K1,K2 & K3 are atomic variables of compound statements

2. Literature Review

2.1 Binary Number System:

The binary number system is a base-2 numeral system, which means it uses only two digits: 0 and 1. It's the foundation of all modern digital electronics and computing systems. In contrast to the decimal system, which uses 10 digits (0 through 9), binary relies on powers of 2. Each digit in a binary number represents a power of 2. Starting from the rightmost digit, each digit's place value doubles as you move left. To convert a binary number to its decimal equivalent, you multiply each digit by its corresponding power of 2 and then add up the results. Converting decimal numbers to binary involves repeatedly dividing the decimal number by 2 and noting the remainders, then reading those remainders from bottom to top to get the binary representation. The binary system's simplicity makes it well-suited for electronic systems since it's easy to represent with switches (on/off), which are the basic building blocks of digital circuits.

In mathematics and in computing systems, a binary digit, or bit, is the smallest unit of data. Each bit has a single value of either 1 or 0, which means it can't take on any other value. Computers can represent numbers using binary code in the form of digital 1s and 0s inside the central processing unit (CPU) and RAM [10,13].

Example: SECRET

S	E	C	R	E	T
18	4	2	17	4	19

Binary code: 10010 100 10 10001 100 10011

2.2 Octal number system:

The octal number system is a numeral system with base-8 which means it uses 8 digits: 0, 1, 2, 3, 4, 5, 6, and 7. It's often used in computing systems, particularly in the past, as it was a convenient way to represent binary data. Each digit in an octal number represents a power of 8. Starting from the rightmost digit, each digit's place value increases by a power of 8 as you move left. To convert an octal number to its decimal equivalent, multiply each digit by its corresponding power of 8 and then add up the results. Converting decimal numbers to octal involves repeated division of the decimal number by 8 and noting the remainders, then reading those remainders from bottom to top to get the octal representation While octal was more prevalent in the past, it's less commonly used today in favor of hexadecimal or binary, especially in computing contexts. However, it's still occasionally encountered in certain applications, such as file permissions in Unix-like operating system.

Octal refers to the numbering system with base-8. It comes from the Latin word for eight. The numerals, 0-1-2-3-4-5-6-7 are used in the octal numbering system. It is frequently used as a shorter representation of binary numbers by grouping binary digits into threes in computing environments. [6,8]

Example:

E	N	C	R	Y	P	T	I	O	N
4	13	2	17	24	15	19	8	14	13

Octal code: 4 15 2 21 30 17 23 10 16 15

2.3 Hexadecimal number system:

The hexadecimal number system is a numeral system, with base-16 which means it uses 16 digits: 0-9 followed by the letters A-F (representing 10 to 15). It's widely used in computing because it provides a suitable way to constitute large binary numbers in a more compact and human-readable or an intelligible format.

Each digit in a hexadecimal number represents a power of 16. Starting from the rightmost digit, each digit's place value increases by a power of 16 as you move left.

To convert a hexadecimal number to its decimal equivalent, multiply each digit by its corresponding power of 16 and then add up the results.

Converting decimal numbers to hexadecimal involves repeated division of the decimal number by 16 and noting the remainders, then reading those remainders from bottom to top to get the hexadecimal representation.

In computing, hexadecimal is particularly useful because each hexadecimal digit corresponds to exactly four binary digits (bits). This one-to-one correspondence makes it easy to represent binary data, such as memory addresses, byte values, or color codes, in a more concise and manageable way. Additionally, hexadecimal is commonly used in programming languages, debugging, and digital communication protocols.

The number system, that has a base value equal to 16 hexadecimal number system. It is also pronounced sometimes as 'hex'. Hexadecimal numbers are represented by only 16 symbols. These symbols or values are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F, each digit representing a decimal value.

Example:

	C	R	Y	P	T	O	L	O	G	Y
	2	17	24	15	19	14	11	14	6	24
Hexadecimal:	2	11	18	15	13	14	11	14	6	18

2.4 ASCII Number System:

The ASCII (American Standard Code for Information Interchange) system is not exactly a number system like binary, octal, decimal, or hexadecimal but, it's a character encoding standard that allocates numerical values to characters. In ASCII, each character is represented by a unique 7-bit binary number (extended ASCII uses 8 bits). Originally developed for telegraphy, ASCII has become the basis for encoding text in computers and communication equipment. The ASCII standard includes codes for letters, numbers, punctuation marks, and control characters, such as carriage return and line feed. Here's a basic ASCII table showing some characters and their corresponding decimal values. While ASCII uses decimal numbers for representation in tables and documentation, it's often more convenient to work with hexadecimal representations, particularly in programming contexts. For example, the letter 'A' in ASCII is represented as 41 in hexadecimal. Because ASCII only covers characters used in English text, it's been superseded by more comprehensive character encoding standards like Unicode, which supports a wider range of characters from various languages and symbol sets. ASCII, a standard data-encoding format for electronic communication between computers assigns standard numeric values to letters, numerals, punctuation marks, and other characters used in computers. In full: American Standard Code for Information Interchange.

Example:

C	O	M	P	U	T	E	R
ASCII: 67	79	77	80	85	84	69	82

P.A. Kameswari et al. [20] solved DLP using pollard Rho algorithm, the cryptosystem based on above DLP useful for transmitting the data securely, but security levels are weak. Surendra, T et al. [21] developed cryptosystem based on ATP and antecedent and consequent rules assigned to the ciphers. In this cryptosystem as the ciphers used already known there is a possibility for attacks. P.A. Kameswari et al. [20] solved DLP using pollard Rho algorithm, the cryptosystem based on above DLP useful for transmitting the data securely, but security levels are weak. Surendra, T et al. [21] developed cryptosystem based on ATP and antecedent and consequent rules assigned to the ciphers. In this cryptosystem as the ciphers used already known there is a possibility for attacks. Surendra, T et al. [22] developed cryptosystem based on ATP and antecedent and consequent rules assigned to the ciphers. In this cryptosystem as the ciphers used already known there is a possibility for attacks.The present developed cryptosystem which is based on Automatic Theorem Proving and new sequent rules in three variables assigned with various number systems overcomes above limitations.

3. Proposed Algorithms:

3.1 Encryption process: [21]

Based on the length of the block, the number of elements in the domain set varies. If block length is r>0, domain set will contain $(26)^r$ number of elements. Here we considered block length 2, so the domain set contain $(26)^2$=676 elements. Consider the domain set as $\{X_1,X_2,\ldots X_{676}\}$where X_1=AA,X_2=AB,…X_{676}=ZZ. Divide the plain text into 'm' blocks with block length k where m>0 and k>0. Label the blocks with the corresponding elements in the domain set which contain $(26)^k$ elements with k=2.Then form the sequent with these blocks and connective symbols {∧,v,⇄,⋔,¤,₳,©,@,ƚ,ö,∀} using ATP and make sure that the statement formula, either single variable or compound formula may contain in antecedent part or consequent or both. After this apply newly defined two and three variables antecedent and consequent rules until to get eliminate all the connective symbols. Here we get various levels of cipher texts. As it involves different levels of cipher text, it is difficult to the attacker to decrypt the plain text. Here the 1st secret is set of number of systems assigned to the sequent rules. The public key the set contain two parts, first part variables to be used in antecedent part while forming first decryption sequent. Similarly, variables in the second part of the public key are to be used in consequent part while forming first decryption sequent. In the public key, [7] these two parts were separated by the symbol ';'. The second secret key is the set of "antecedent and consequent rules used in order to get level-1 to final level cipher texts". The second secret key contains the order of the connective symbols removed in the encryption sequent's. In the second secret key one connective symbol is to be applied to two variables or two statement formulas only in the process of decryption. The public key is set of "variables X_j with $1\leq j\leq(26)^2$ in the final encryption sequent".

3.2 Encryption algorithm:

1. Divide the plain text into finite number of blocks say m, where each block contain 'k' number of alphabets (k>0). If any block contain less than k number of numerals then make it k number block by filling with dummy alphabet say x. we can fill with any other alphabet by our choice.

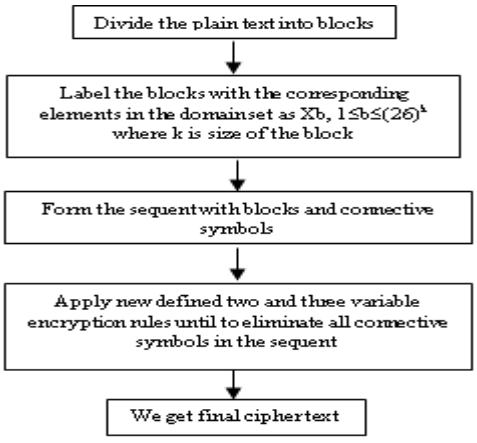
2. Label these blocks as with the elements in the domain set, where the domain set contain X1,X2,…..Xr where $r=26^k$ the number of elements in the domain set which we use for plain text labeling.
3. Form sequent with these blocks in such way that can apply defined two or three variables sequent rules.

4. Then apply sequent rules, we get various levels of ciphers texts.

5. Repeat the process until all the connective symbols will get eliminated and then we get final cipher text.

6. Here public key is connective symbols in order wise eliminated and private key is set of two variable sequent rules assigned ciphers and Three variable sequent rules assigned with different number systems. Also through private key will agree block length.

Encryption flow chart:



3.3 Decryption process:

The cipher text obtained from the sender have to divide into m number blocks where each block contain 'k' number of alphabets (k>0). Label these blocks with Xj, $1 \leq j \leq (2)^{26}$, using the public key [7]. Then form the decryption sequent with these blocks secret key 2. Then apply two and three variable decryption rules by following secret key 1 and secret key 2. The connectives in the secret key are used in reverse order i.e., from backward direction to decode the cipher text. The implications in the secret key are used from the right and 'c followed by connective symbol represents rules that has to be applied in decryption consequent part. Similarly, 'a followed by connective symbol' represents that rule to be applied in decryption antecedent part'. With one connective symbol in the secret key, compound statement is formed by taking two variables or two compound statements or one variable and compound statement by considering the order. The process is repeated until all the connectives are used in the secret key. In this process we get required plain text [16,24].

3.4 Decryption algorithm:

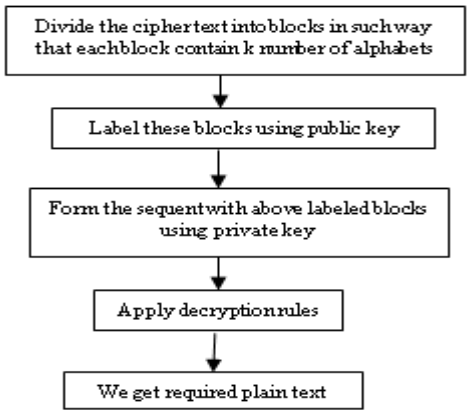
1. Divide the cipher text into m number of blocks as block length agreed through secret key.

2. Label these blocks using public key.

3. Form the sequent with these using another public key.

4. Apply Decryption process using public and private keys then we get required plain text.

Decryption flow chart



4. Implementation of Encryption and Decryption:

Symbol	Name
X@Y	Jelly cipher
X©Y	Tree fence cipher
(X¤Y)Ⱥ Z	Octal system
(XƔY)∀Z	ASCII system
(XƵY) ൿ Z	Hexa decimal system
a-0, b-1, c-2, z-25	Alphabets and its values in encryption sequent
$\Rightarrow^{Sn}$	n- decryption sequent
a-connective	connective symbol used in antecedent part
c-connective	connective symbol used in consequent part

4.1 Implementation 1. [4,5]

Plain text: **CHANDRAYAN IS READY FOR LAUNCHING**

Divide the this plain text as 2 letter blocks as 'CH|AN|DR|AY|AN|IS|RE|AD|YF|OR| LA|UN|CH|IN|GX' where X_{62}= CH, X_{14}=AN, X_{122}=DR, X_{25}=AY, X_{14}=AN, X_{253}=IS, X_{473}=RE, X_4=AD, X_{656}=YF, X_{408}=OR, X_{313}=LA, X_{560}= UN, X_{86}= CH, X_{248}=IN,X_{206}=GX. So divided plain text blocks equivalent to ($X_1|X_2|X_3|X_4|X_5|X_6|X_7|X_8|X_9|X_{10}$). For the first sequent with these variables as [(X_{248}ƧX_{560})ጠX_{408}]ʌX_4ʌ [(X_{253}¤X_{25}) ȺX_{14}] $\Rightarrow^{S1}$ (X_{206}©X_{86})v(X_{313} @X_{656})v X_{473}v [(X_{14}ƅ X_{122})∀X_{62}]. Then apply first 'rule ʌ⇒' and 'rule⇒ v' we get [(X_{329}ƧX_{641}) ጠX_{489}],X_{111}, [(X_{334} ¤X_{106}) Ⱥ X_{121}] $\Rightarrow^{S2}$ (X_{220}©X_{185}), (X_{642}@X_{131}) , X_{181} , [(X_{471}ƅ X_4)∀X_{388}] where X_{329} =LQ, X_{641} =XQ, X_{489} =RU, X_{111}=DG, X_{334}=LV, X_{106}=DB, X_{121}=DQ, X_{220}=HL, X_{185}=GC, X_{642}=XR,X_{131}=EA, X_{181}=FY, X_{471}=RC, X_4 =AD, X_{388}=NX. Now again apply 'rule Ƨ ⇒' now the above sequent we get X_{323}, X_{111}, [(X_{334} ¤ X_{106}) Ⱥ X_{121}] $\Rightarrow^{S3}$ (X_{220} © X_{185}),(X_{642}@X_{131}), X_{181}, [(X_{471}ƅX_4)∀X_{388}] , $X_{479}X_{327}$ where X_{323}=LK, X_{479} =RK, X_{327} =LO, now again apply 'rule ¤ ⇒' now the above sequent we get X_{323}, X_{111} , $X_{390}X_{106}X_{125}$ $\Rightarrow^{S4}$ (X_{220}©X_{185}), (X_{642} @ X_{131}), X_{181}, [(X_{471}ƅX_4) ∀ X_{388}], $X_{479}X_{327}$ where X_{390} =NZ, X_{106} =DB, X_{125}=DU now again apply 'rule⇒© ' on the above sequent then we get X_{323}, X_{111}, $X_{390}X_{106}X_{125}$ $\Rightarrow^{S5}$ $X_{90}X_{215}$,(X_{642}@X_{131}) , X_{181}, [(X_{471} ƅX_4) ∀ X_{388}], $X_{479}X_{327}$ where X_{215} =HG, X_{90} =CL, now again apply 'rule⇒@' on the above sequent then we get X_{323}, X_{111}, $X_{390}X_{106}X_{125}$, X_{347}⇒^{S6} $X_{90}X_{215}$,X_{182} ,X_{181},[(X_{471}ƅX_4)∀X_{388}] , $X_{479}X_{327}$ where X_{182} =FZ, X_{347} =MI now again apply 'rule⇒ƅ ' on the above sequent then we get X_{323}, X_{111}, $X_{390}X_{106}X_{125}$, X_{347} , ($X_{385}^{(L)}$ $X_{150}^{(X)}$) $\Rightarrow^{S7}$ $X_{90}X_{215}$, X_{182} ,X_{181}, ($X_{107}^{(1)}$ $X_{514}^{(X)}$) (X_{96} $X_{150}^{(B)}$) , $X_{479}X_{327}$ where $X_{107}^{(1)}$ $X_{514}^{(X)}$ = DC1 STX $X_{385}^{(L)}$ $X_{150}^{(X)}$ = NUL ETX X_{96} $X_{150}^{(B)}$ = CR ETB stop the processes since all the connective symbols where eliminated in the last sequence so final level cipher is LQDGNZDBDU MINULETX⇒CLHGFZFYDC1STXCRETBR KL O. The public key is {X_{323},X_{111},$X_{390}X_{106}X_{125}$,X_{347}, $X_{107}^{(1)}X_{514}^{(X)}X_{385}^{(L)}X_{150}^{(X)}$;$X_{90}X_{215}$,$X_{182}$, X_{181}, $X_{107}^{(1)}$ $X_{514}^{(X)}$ X_{96} $X_{150}^{(B)}$,$X_{479}X_{327}$ } and secret key 1 is {@-Jelly, ©-Tree fence, ¤,Ⱥ-Octal, ƅ, ∀-ASCII, Ƨ,ጠ-Hexa} and secret key 2 is {a**ʌ,cv,a**Ƨ**,a**¤**,c**©**,c**@**,c**ƅ}.

5. Results and Discussion:

Fig. 1: The execution time of Encryption

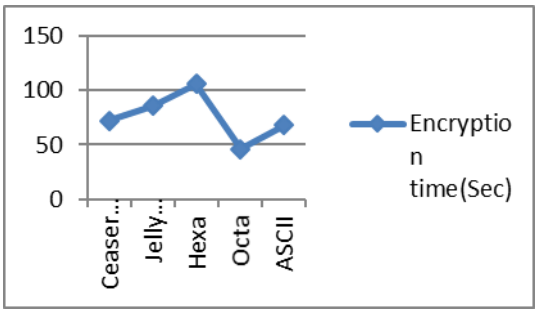


Fig. 2: The execution time of Decryption

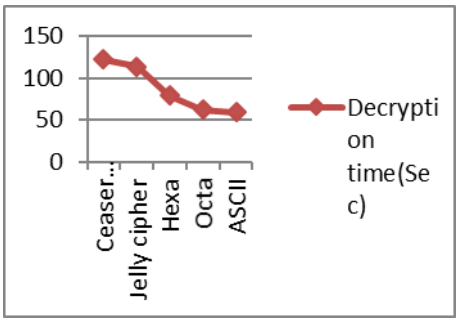
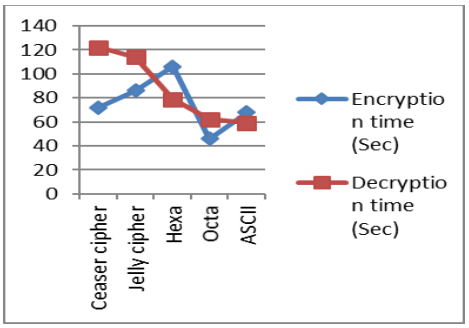


Fig. 3: The execution time of Encryption & Decryption



5. Cryptanalysis:

New cryptosystems with automatic theorem proving with novel encryption and decryption rules using three or more variables assigned to different methods can be developed [3] in future and these rules can be extended for n variables also and we can apply programming techniques, so that more data also we can do encryption and decryption easily.

6. Acknowledgements:

The authors would like to express their gratitude for the support extended by the Department of Mathematics, GSS, and GITAM Deemed to be University.

Refrences

[1] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, "Hand book of Applied Cryptography." CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.
[2] Bhishma Rao, "A text of Mathematical Foundations of Computer Science", SciTech Publications (India) Pvt Ltd., ISBN- 10: 8183710433.
[3] Douglas R. Stinson "Cryptography theory and practice" Second edition.
[4] Geoff Sutcliffe, "Automated Theorem Proving: Theory and Practice A Review", AI Magazine Volume 23 Number 1 (2002) (© AAAI).
[5] Gerhard Frey "The arithmetic behind cryptography" AMS volume 57, Number 3.
[6] Hans Delfs Helmut Knebl "Introduction to cryptography" Principles and its Applications, second edition.
[7] Harry Yosh "The key exchange cryptosystem used with higher order Diophantine equations" IJNSA VOL.3, 15. No.2, March 2011.
[8] I. Niven, H.S. Zuckerman and J.H. Silverman "An Introduction to the Theory of Numbers", 5th ed., John Wiley and Sons, New York, 1991.
[9] J. Buchmann "Introduction to cryptography", Springer Verlag 2001.
[10] J.P. Tremblay & R. Manohar, "A text book of Discrete Mathematical Structures with Applications to Computer Science', McGraw Hill Education (India) Edition 1997.
[11] Keith M. Martin, Rei Safavi-Naini, Huaxiong Wang and Peter R.Wild "Distributing the encryption and decryption of a block cipher".
[12] K.H. Rosen, "Elementary number theory and its applications" Third edition, Addison- Wesley.
[13] Menzes A. and Vanstone S. "Hand book of applied cryptography", The CRC-Press series of Discrete Mathematics and its Applications CRC-Press, 1997.
[14] Neal Koblitz "A course in number theory and cryptography" ISBN 3-578071-8, SPIN 10893308.
[15] Peter J. Smith and Michael J.J. Lennon, "A New Public Key System" LUC Partners, Auckland UniServices Ltd, The University of Auckland, Private Bag92019m Auckland, New Zealand.
[16] Phillip Rogaway Mihir Bellare John Black Ted Krovetz "OCB: A block-cipher mode of operation for efficient authenticated encryption".
[17] P.Rogaway, M-Bellare, J. Black,T-Korvetz "A Block Cipher mode of operation for efficient authenticated encryption" Eighth ACM conference on computer and communication security (CCS-8) ACM Press, 2001.
[18] Serge Vaudenay "A classical introduction to cryptography applications for communication security" Springer International Edition.
[19] Song Y. Yan, "Number Theory for computing", 2nd edition, Springer, ISBN: 3- 540-43072-5.
[20] Surendra Talari & P. Anuradha Kameswari, Pollard RHO algorithm implemented to Discrete Log with Lucas sequences, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN:2321-8169 Volume: 4, Issue: 3.
[21] Surendra Talari, S.S. Amiripalli, P. Sirisha, D.S. Kumar and V.K. Deepika, An Improved Cipher Based Automatic Theorem Proving Technique for encryption and Decryption, "Advances in Mathematics: Scientific Journal", page numbers 3121-3134, volume 9/5, June, 2020.

[22] Surendra Talari, K.K. Sowjanya, G. Yojana, and V. Prasad, New Cryptosystem Using Enhanced Automatic Theorem Proving and Enhanced Ciphers, "Journal of Theoretical and Applied Information Technology", pa numbers 6434-6443, volume 101/20, October, 2023.
[23] W. Diffi and M. E. Helman "New directions in Cryptography." IEEE Transactions on Information theory, 22, 644654, 1976.
[24] William Stallings "Cryptography and network security principals and practice" 5th ed.